RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: LAB2-M01

Applying and Adapting the CISA Zero Trust Maturity Model to the Enterprise

Jason Garbis

Founder and CEO
Numberline Security
https://www.linkedin.com/in/jasongarbis/

Jerry Chapman

Director of Identity Services and Solutions
Verinext
https://www.linkedin.com/in/jerrychapman/

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Lab Exercise Structure

- Your table has an assigned topic from one of the pillars
- You'll be focused on that topic area
- Feel free to switch tables if you'd like
- Challenge Mode: Choose a topic you're unfamiliar with!

Agenda

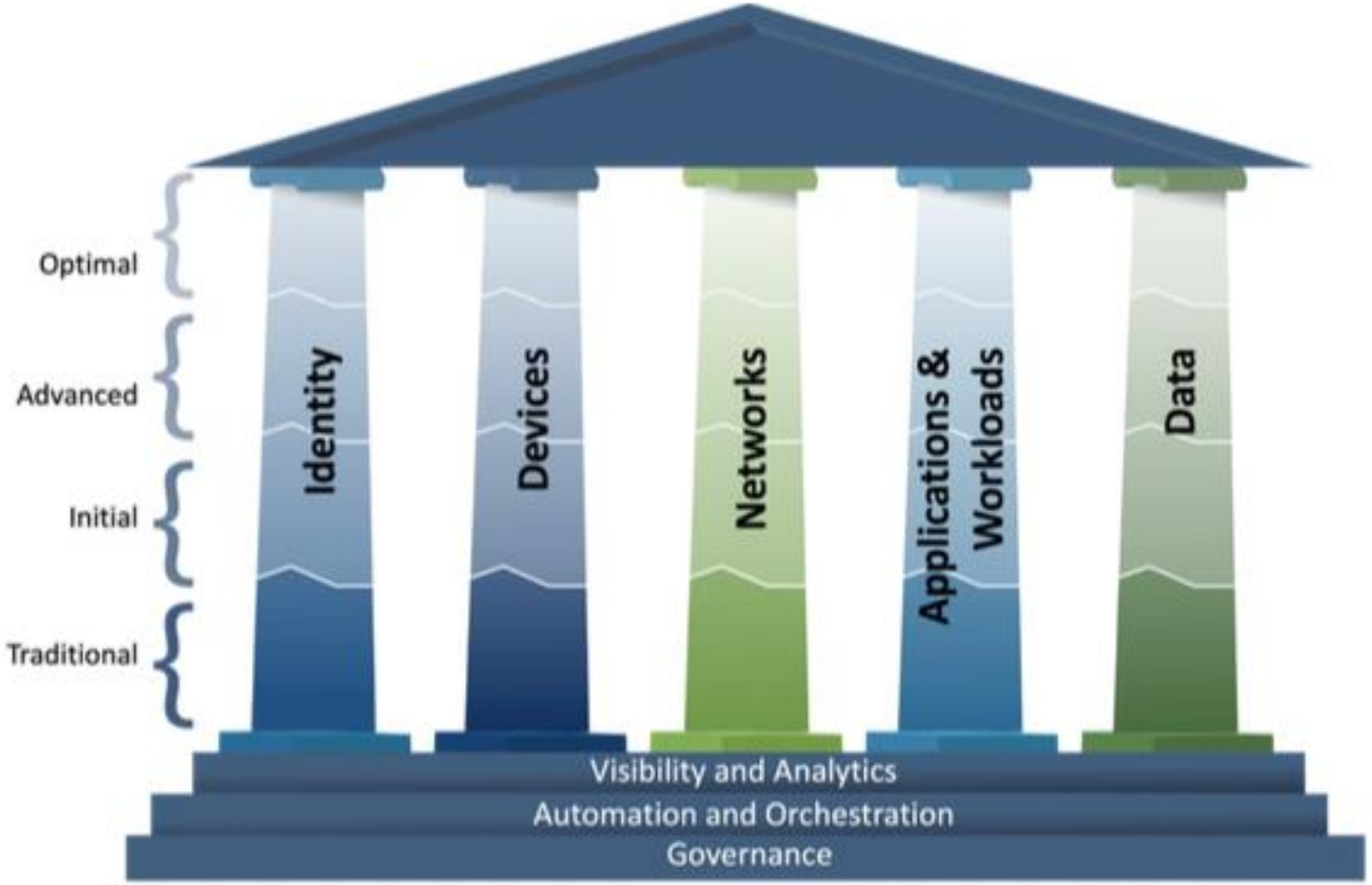
- Topic 1: (re) Introducing the CISA Zero Trust Maturity Model
  - Presentation
  - Exercise: Critiquing the CISA ZTMM
- Topic 2: ZTMM+: The Enhanced and Extended Zero Trust Maturity Model
  - Presentation
  - Exercise: Applying ZTMM+ to your Enterprise
- Topic 3: : Improving Your Maturity Level (Making the Assessment Actionable)
  - Presentation
  - Exercise: Identifying Next Steps (Initiatives for Improvement)
- Summary, Takeaways, and Actions You Should Take

Audience Poll: Familiarity with CISA ZTMM?

RSAC 2025 Conference

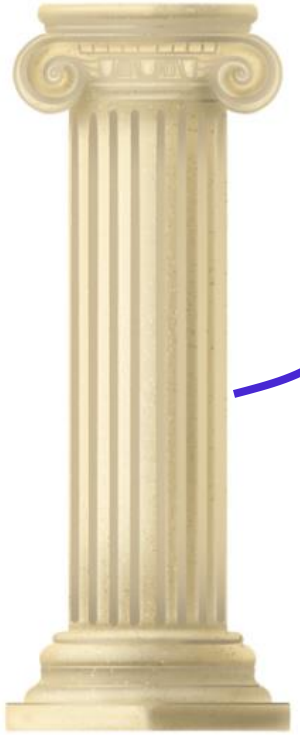
Part 1: (re) Introducing the CISA Zero Trust Maturity Model

(Re) Introducing the CISA Zero Trust Maturity Model



- 5 Pillars
- 3 Cross-Cutting Capabilities
- 4 Maturity Levels
- 40 Functions

CISA ZTMM Structure



Pillars

Functions
Authentication
Identity Stores
Risk Assessments
Access Management
Visibility and Analytics
Automation and Orchestration
Governance

Functions
(example: from Identity pillar)

Traditional	Initial	Advanced	Optimal
• ----------	• ----------	• ----------	• ----------
• ----------	• ----------	• ----------	• ----------
• ----------	• ----------	• ----------	• ----------

Maturity Levels
(defined for each function)

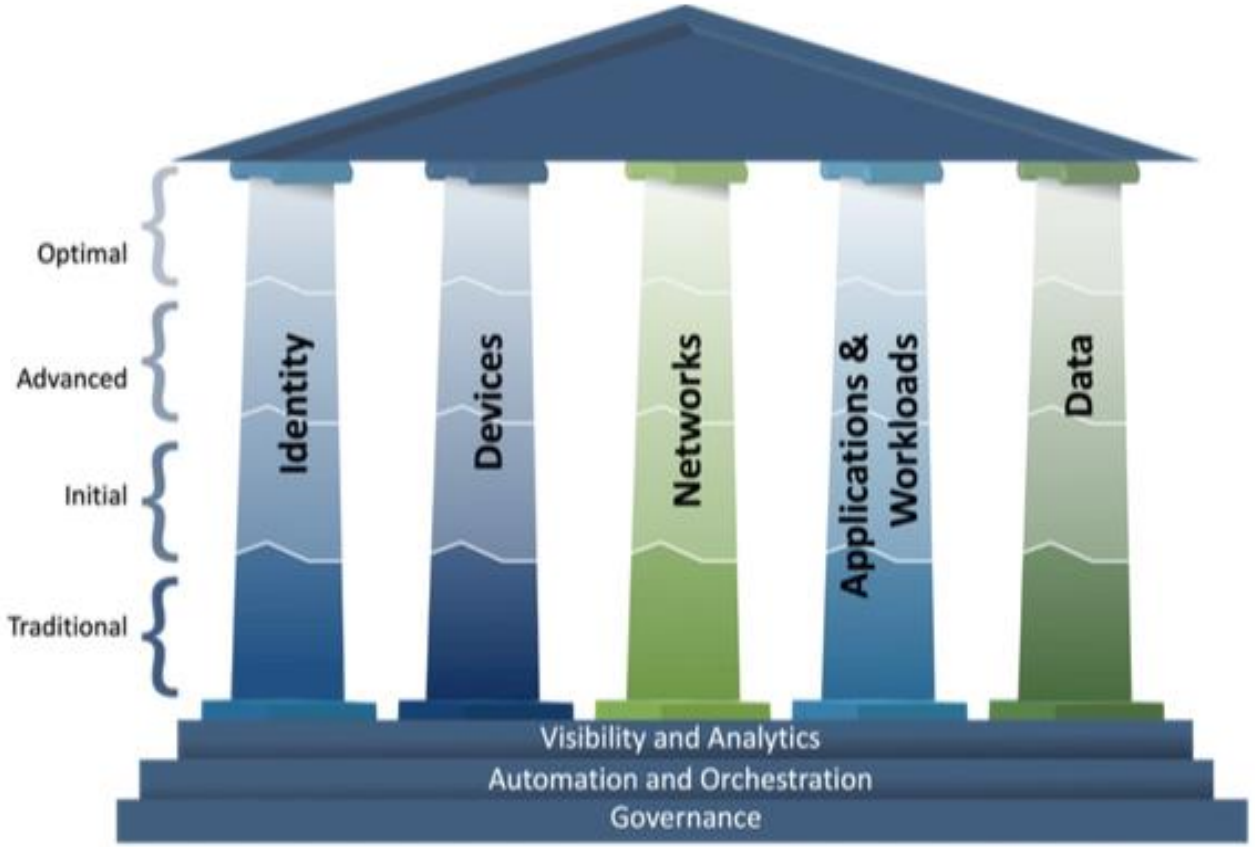
Sample Function: Devices: Policy Enforcement and Compliance Monitoring

Traditional	Initial	Advanced	Optimal
Agency has limited, if any, visibility (i.e., ability to inspect device behavior) into device compliance with few methods of enforcing policies or managing software, configurations, or vulnerabilities.	Agency receives self-reported device characteristics (e.g., keys, tokens, users, etc., on the device) but has limited enforcement mechanisms. Agency has a preliminary, basic process in place to approve software use and push updates and configuration changes to devices.	Agency has verified insights (i.e., an administrator can inspect and verify the data on device) on initial access to device and enforces compliance for most devices and virtual assets. Agency uses automated methods to manage devices and virtual assets, approve software, and identify vulnerabilities and install patches.	Agency continuously verifies insights and enforces compliance throughout the lifetime of devices and virtual assets. Agency integrates device, software, configuration, and vulnerability management across all agency environments, including for virtual assets.

RSAC 2025 Conference

Exercise 1: Critiquing the CISA ZTMM

Exercise 1: Critiquing the CISA ZTMM



The core of the CISA Model is included in Appendix A of your Workbook
Also, there is one full printed copy on each table

- What's missing, off-target, or could be improved in your pillar?
- Small group discussion (10 Minutes)
- Sharing and facilitated discussion (10 Minutes)
- Guidance to get you started:
  - How well do these functions align with your organizations' teams and responsibilities?
  - Do you see any functions missing from this pillar?
  - In your pillar, pick 1 function's maturity progression…how well does it reflect your experience?

NUMBERLINE SECURITY

RSAC 2025 Conference

Exercise 1: Sharing & Discussion

RSAC 2025 Conference

Part 2: ZTMM+: The Enhanced and Extended Zero Trust Maturity Model

CI
SA

CISA ZTMM is a Great Starting Point

ZTMM+

- Clearly Defined every Pillar Function
- Clarified 20 function maturity pathways
- Added 7 entirely new functions
- Developed a Structured Methodology for Maturity Assessments
  - Decomposed functions into simple questions, each with maturity pathway
  - Structured process for assessing

ZTMM+ Functions

Identity Pillar

- User Authentication
- NPE Authentication
- Identity Stores
- Identity Store Roles and Attributes
- Risk Assessments
- Access Management
- Visibility and Analytics
- Automation and Orchestration
- Governance

Devices Pillar

- Policy Enforcement & Compliance Monitoring
- Asset & Supply Chain Risk Management
- Resource Access
- Device Threat Protection
- Device Lifecycle Management
- Visibility and Analytics
- Automation and Orchestration
- Governance

Networks Pillar

- Network Segmentation
- Network Traffic Management
- Traffic Encryption
- Network Resilience
- Secure Internet Access
- Visibility and Analytics
- Automation and Orchestration
- Governance

Applications and Workloads Pillar

- Application Access Authorization
- Application Threat Protections
- Private Application Access
- Secure Application Development and Deployment Workflow
- Application Security Testing
- SaaS Application Security
- Visibility and Analytics
- Automation and Orchestration
- Governance

Data Pillar

- Data Inventory Management
- Data Categorization
- Data Availability
- Data Access
- Data Loss Prevention
- Data Encryption
- Data Lifecycle Management
- Visibility and Analytics
- Automation and Orchestration
- Governance

Example: Identity : Authentication Function

Traditional	Initial	Advanced	Optimal
Agency authenticates identity using either passwords or multi-factor authentication (MFA) with static access for entity identity	Agency authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g., locale or activity).	Agency begins to authenticate all identity using phishing-resistant MFA and attributes, including initial implementation of password-less MFA via FIDO or PIV	Agency continuously validates identity with phishing-resistant MFA, not just when access is initially granted.

- Split and Enhanced CISA's Authentication function
  - User Authentication : Refocused, and clarified maturity pathway
  - Non-Person Entity (NPE) Authentication : New function

User Authentication

How human users authenticate for access to enterprise systems, via interactive logins. Includes traditional usernames / passwords, passwordless, biometric authentication. Includes authentication into identity providers for SSO, as well as authentication directly into enterprise systems and applications.

How do users authenticate?			
Traditional Username and Password only, No MFA	**Initial** Some MFA (SMS or email)	**Advanced** Some phishing-resistant MFA (FIDO2, biometric) or passwordless	**Optimal** Mostly phishing-resistant MFA (FIDO2, biometric) or passwordless
How are Privileged Admin Accounts authenticated?			
Traditional Same account as regular, daily login with username / password	**Initial** Separate Account, username / password, MFA required	**Advanced** PAM Solution in place, username / password checkout and MFA required	**Optimal** PAM Solution, Credentials automated and cycled, MFA enforced.
What methods are used for Single Sign-On (SSO) in your environment?			
Traditional Users authenticate with traditional username / password. Little to no SSO in place	**Initial** Users authenticate mostly via username / passwords, with initial usage of SSO for selected applications	**Advanced** SSO in place for many applications, using standards (e.g. SAML) or Federated Identities	**Optimal** Broadly deployed SSO, widespread usage of Federated Identities and standards such as OIDC authentication

NPE Authentication

Non-Person Entity (NPE) authentication into the enterprise environment. NPEs can include service accounts, workloads, and machine identities.

How do Service Accounts authenticate?			
Traditional Implicit trust, or basic password-based authentication at access time.	**Initial** Certificate-based authentication, or usage of password vaults for static credential storage	**Advanced** Active PAM system management of service credentials, with password rotation	**Optimal** Ephemeral certificates or secrets, with retrieval of Secrets through Secrets Management environment. Or, standards-based workload identity (e.g SPIFFE)

Full ZTMM+ Overview

RSAC 2025 Conference

Exercise 2:
Applying ZTMM+ To Your Enterprise

Exercise 2: Applying ZTMM+ To Your Enterprise

- Individual Work: (5 Minutes)
  - Select one function within your pillar
  - For each function attribute shown, evaluate your enterprise's current maturity
- Small group discussion (10 Minutes)
- Sharing and facilitated discussion (10 Minutes)
- Guidance:
  - For each question, select the maturity level that best fits your enterprise as it stands today
  - If you don't know, who in your enterprise could you ask?
  - Are there aspects of it that don't quite align?

RSAC 2025 Conference

Exercise 2: Sharing & Discussion

RSAC 2025 Conference

Part 3: Improving Your Maturity Level (Making the Assessment Actionable)

Zero Trust Maturity is Not Soccer (Football)

Improving Maturity is Important…. But it Shouldn't Be Your Primary Goal

- Remember
  - The primary goal of a Zero Trust initiative is to deliver value to the business
- Improving maturity is important
  - It provides you with more (and better) security capabilities
    - With which to deliver value to the business
- A Zero Trust Maturity Model is a great guide for this

Having Said That…
Improving Maturity is important

- Choose an appropriate target maturity level for each function
- Keep in mind that *Optimal* is not necessarily the target for all functions
- Your target should be chosen based upon
  - Risk tolerance
  - Budget
  - Resources and other commitments
  - Opportunity costs

Example

User Authentication: Current Maturity

How do users authenticate?			
Traditional Username and Password only, No MFA	**Initial** Some MFA (SMS or email)	**Advanced** Some phishing-resistant MFA (FIDO2, biometric) or passwordless	**Optimal** Mostly phishing-resistant MFA (FIDO2, biometric) or passwordless
How are Privileged Admin Accounts authenticated?			
Traditional Same account as regular, daily login with username / password	**Initial** Separate Account, username / password, MFA required	**Advanced** PAM Solution in place, username / password checkout and MFA required	**Optimal** PAM Solution, Credentials automated and cycled, MFA enforced.
What methods are used for Single Sign-On (SSO) in your environment?			
Traditional Users authenticate with traditional username / password. Little to no SSO in place	**Initial** Users authenticate mostly via username / passwords, with initial usage of SSO for selected applications	**Advanced** SSO in place for many applications, using standards (e.g. SAML) or Federated Identities	**Optimal** Broadly deployed SSO, widespread usage of Federated Identities and standards such as OIDC authentication

Example Part 2

- Previous slide shows a typical organization's maturity for this function
- Some initiatives to support moving forward:
  - Move to Authentication Application with PUSH notifications and Biometric authentication on the device
  - Move to Passkeys across as many devices as possible
  - Create Admin accounts and separate functionality
  - Develop plan to support Legacy application modernization.

RSAC 2025 Conference

Exercise 3: Identifying Next Steps (Initiatives for Improvement)

Exercise 3: Identifying Next Steps

- Individual Exercise (5 Minutes)
  - Select one function within your pillar for improvement,
  - Identify 3 things to improve its maturity, and for each note
    - Potential obstacles
    - Anticipated “side” benefits
    - Related security, IT, process changes that would increase effectiveness
- Small group discussion (10 Minutes)
- Sharing and facilitated discussion (10 Minutes)
- Guidance:
  - The “delta” between each maturity level indicates what needs to improve

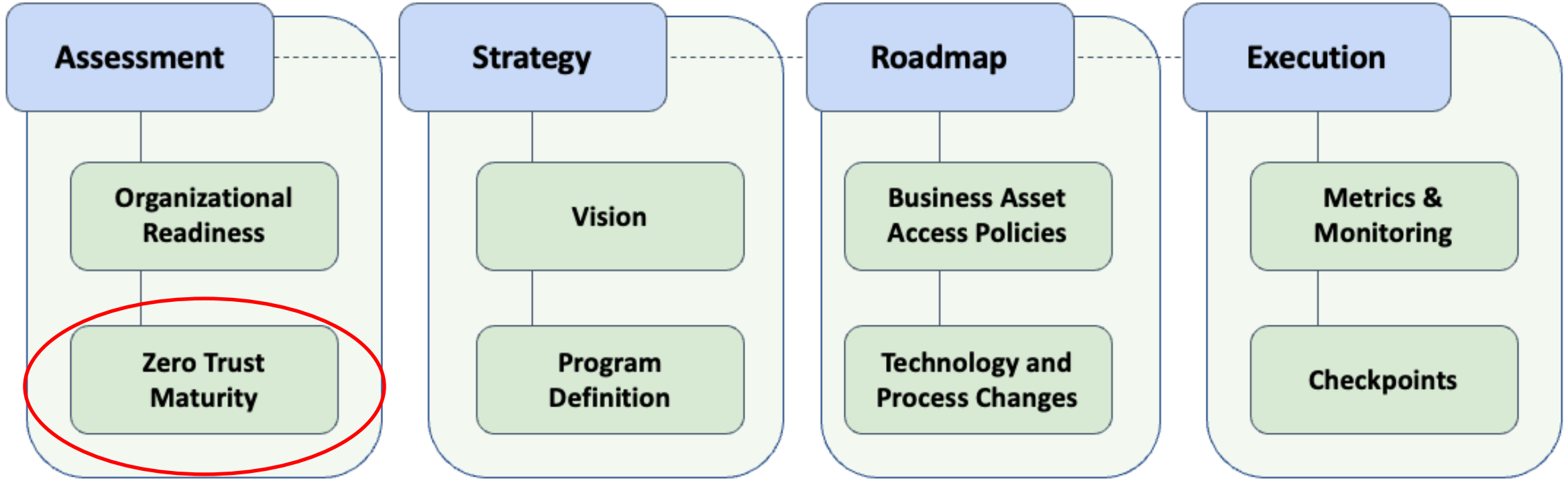
RSAC 2025 Conference

Exercise 3: Sharing & Discussion

RSAC 2025 Conference

Summary and Takeaways / Next Steps

Maturity Assessments are part of an Overall Zero Trust Initiative Blueprint



Apply What You've Learned Today (1)

- Next week you should:
  - Assemble your team, and begin planning your maturity assessment
- Within the next month:
  - Complete your maturity assessment
  - Develop a draft Zero Trust vision, and program structure
  - Research & identify business priorities and initiatives to support with Zero Trust

Apply What You've Learned Today (2)

- Within 3 months:
  - Validate and being resource planning for your Zero Trust initiative
  - Pilot projects for specific business assets, and new access policies
  - Identify processes and governance systems to be improved
- Within six months you should:
  - Expand Zero Trust initiative to a broader set of business assets
  - Deliver end user and business value
  - Procure initial set of necessary technologies to advance your capabilities
  - Re-evaluate your maturity to assess improvements (6+ months)

RSAC 2025 Conference

Many Voices.
One Community.

Thank You!

Jason Garbis

Founder and CEO
Numberline Security
https://www.linkedin.com/in/jasongarbis/

Jerry Chapman

Director of Identity Services and Solutions
Verinext
https://www.linkedin.com/in/jerrychapman/